

# 國立政治大學物聯網設備安全指引

民國 111 年 10 月 31 日資訊安全暨個人資料保護推行委員會第 18 次會議通過

- 一、本指引所稱物聯網設備係指處理公務具網路連線功能之設備，包含無線網路基地台/無線路由器、網路攝影機、網路印表機、門禁設備、環控系統、數位撥放器、無人機等。
- 二、單位應建立物聯網設備管理清冊，並至少每年更新一次。
- 三、設備應具備安全性更新機制，以維持設備之整體安全性。
- 四、設備應具備身分驗證機制，不得使用廠商預設帳密及弱密碼，應**變更預設帳號密碼**，密碼長度應至少 8 碼，並取英文字母大小寫、數字與特殊符號其中 2 種要素之組合。
- 五、設備應關閉不必要之網路連線及服務，依業務需求設定適當網路存取限制；無需對外開放連線者，得以防火牆限制僅供內部連線。
- 六、若設備無法落實本指引第三、四、五條之安全控管規範，應建立補償性管控機制並限制網際網路連線能力，加強存取控制或進行網路連線行為監控。若設備存在已知弱點且無法修補或更新，應訂定汰換期程。
- 七、依行政院規定，禁止使用大陸廠牌資通訊設備。
- 八、設備於採購前，應依據本指引進行評估及測試。
- 九、採購物聯網設備時，得優先採購取得資安標章之物聯網設備，且應與設備供應商簽訂資訊安全相關協議，其內容得包含服務承諾、安全性更新年限、主動通報設備已知資安漏洞並提出相關應變處置方案等事項，以明確約定相關責任。
- 十、針對本校出租場域，應於委外契約或場地租借使用規定，明訂不得使用危害國家資安之產品（如大陸廠牌軟體、硬體及服務）。